

Improvements about processing of measurement results in quantum repeater*

Kenichiro Furuta[†]

Corporate Research and Development Center, Toshiba Corporation

In quantum repeater protocols, measurements are performed in multiple relay points. Classical communications are used to convey the measurement results. It is important to improve the way of conveying the measurement results so that EPR pairs are not affected by noises during classical communications. One solution is execution in the blind mode[1]. In the blind mode, correction operations of multiple ES operations and multiple EPP operations are performed in a lump after EPR pairs are shared between the sender and the receiver. That is, the following quantum operations are performed without performing correction operations of the former quantum operations. The protocol in the conventional blind mode[1] uses concatenated CSS codes. Therefore, the number of qubits gets large as the communication distance gets long.

This paper proposes quantum repeater protocols which can be executed in the blind mode and can be constructed by using CSS codes of single encoding. This result shows that posterior processing can reduce the size of encoded states in some cases. Additionally, the results of this paper show that posterior processing can improve performance of error corrections in some cases. The proposed protocol with single encoding can correct large errors by setting some assumptions. In contrast, blind mode with single encoding can deal with small errors if propositions in this paper are not used. The key ideas in posterior processing are decomposition of errors and computations for comparing EPR pairs of different length.

I. INTRODUCTION

Quantum repeater protocols[1–12] are proposed as methods for generating long EPR pairs. Entanglement Swapping(ES) and Entanglement Purification Protocol(EPP)[13][14] are key components of quantum repeater protocols. Generated EPR pairs can be used for the quantum teleportation[15].

In order to realize quantum repeater protocols in realistic noises, various approaches are taken[1–12]. Some papers try to build abstract protocols without depending on specific materials[1, 2, 7–12]. Among them, some methods[1][11] could achieve small waiting times. That is, all quantum operations can be performed without waiting for arrival of measurement results of the former operations. One of the protocols which could achieve small waiting times is blind mode execution of quantum repeater protocols[1].

A viewpoint of the way of classifying abstract protocols is considering parts of improvements in each protocol. Some protocols[10–12] concentrate focus on the way of encoding so that a small number of measurements on specially encoded states lead to changes which correspond to multiple ES operations and EPP operations. For example, measurements on cluster states[16] are used in [11]. Some protocols[1] concentrate focus on the way of processing of measurement results. In the blind mode[1], it is shown that correction operations which reflect measurement results can be performed later by revising posterior processing of measurement results. This paper studies the protocols which mainly focus on posterior processing.

This paper mainly focuses on posterior processing of measurement results as well as [1] and improve the way of posterior processing in [1]. The main purpose of this paper is not building quantum repeater protocols as an overall protocol, but proposing the efficient way of posterior processing of measurement results. In quantum repeater protocols, measurements are performed in multiple relay points. Besides, quantum states after measurements correspond to measurement results. So, we have to perform correction operations which reflect probabilistic measurement results in multiple relay points. Classical communications are used for conveying measurement results. An important task in building quantum repeater protocols is conveying measurement results by avoiding effects of noises on quantum states during waiting time of classical communications. One solution is to perform correction operations of multiple ES and EPP in a lump after EPR pairs are shared between the sender and the receiver. The quantum repeater protocol based on these directions is blind mode[1]. The protocol in [1] uses concatenated CSS codes. Therefore, the number of qubits gets large as the communication distance gets long. This paper proposes quantum repeater protocols which can be executed in the blind mode and can be constructed by using CSS codes of single encoding. Additionally, the proposed protocol with single encoding can correct large errors by setting some assumptions. In contrast, the simple blind mode with single encoding can deal with small errors if propositions in this paper are not used. The relationship between the proposed methods and the conventional methods can be summarized as follows.

- Proposed method:

This method can correct large errors with single encoding by using the proposition about posterior processing.

* A footnote to the article title

[†] kenichiro.furuta@toshiba.co.jp

- Conventional blind mode with single encoding:
This method can correct only small errors.
- Conventional blind mode with concatenated codes:
Although this method can correct large errors, this method needs a large number of qubits.

Therefore, the results of this paper show that posterior processing can improve performance of error corrections in comparison with conventional blind mode with single encoding. In other words, the results of this paper show that posterior processing can reduce the size of encoded state in comparison with conventional blind mode with concatenated coding. The key ideas in posterior processing are decomposition of errors and computations for comparing EPR pairs of different length, as described in the followings.

II. QUANTUM REPEATER

In this section, we explain the quantum repeater protocol which uses CSS codes in EPP operations[14]. The paper of the blind mode[1] seems to use CSS codes in EPP operations. Since this section does not consider the blind mode, corrections operations in ES and EPP are performed before the next ES operations and EPP operations are performed. We have to note that, in the case of not using blind mode, we can use CSS codes of single encoding since errors are corrected frequently by using classical communications during protocols and errors are not accumulated. In contrast, in the case of the blind mode, we have to use concatenated codes if we do not use special posterior processing which are proposed in this paper.

A. Whole figure of the protocol

In the quantum repeater protocol, operations of ES are used for connecting EPR pairs and operations of EPP are used for increasing fidelity of EPR pairs. Then, long EPR pairs of high fidelity are generated. We assume that two EPR pairs are connected by one-time execution of ES. Let $N - 1$ be the number of relay points. Let γ be the number of executions of ES operation and EPP operation. Then, these parameters satisfy the relationship of $N = 2^\gamma$. Let x be the order of execution of ES and EPP. That is, ES which is executed first is called ES at $x=1$ and EPP which is executed first is called EPP at $x=1$. ES which is executed last is called ES at $x=\gamma$ and EPP which is executed last is called EPP at $x=\gamma$. There are $N - 1$ relay points between the sender A and the receiver B , which are represented as C_1, C_2, \dots, C_{N-1} . A and B are represented as C_0 and C_N , respectively.

- In each relay point, C_i ($i = 0, \dots, N - 1$), EPR pairs are generated. We have to note that n EPR pairs are generated at each relay point since CSS codes of length n are used with single encoding.

- One side of each EPR pair is sent to the adjacent relay points C_{i+1} . These transmissions are called quantum state transmissions.
- From $x = 1$ to $x = \gamma$, repeat the following operations.
 - Operations of ES are performed on relay points, $C_{k \times 2^{x-1}}$ ($k = 1, 2, \dots, N/2^{x-1} - 1$) except $C_{2^x}, C_{2 \times 2^x}, \dots, C_{N-2^x}$.
 - By using classical communications, measurement results are sent to both edges of EPR pairs which are generated by the ES operation.
 - Correction operations which reflect measurement results are performed on both edges of EPR pairs which are generated by ES operations. These operations lead to generation of EPR pairs which are shared between $C_{k \times 2^x}$ and $C_{(k+1)2^x}$ for $k = 0, \dots, N/2^x - 1$.
 - Operations of EPP are performed between $C_{k \times 2^x}$ and $C_{(k+1)2^x}$ for $k = 0, \dots, N/2^x - 1$. These operations lead to EPR pairs of higher fidelity. In EPP operations, measurement operators of CSS codes are used for outputting syndromes[14]. Since errors are corrected at every EPP operations and errors are not accumulated, we can use CSS codes of single encoding at every EPP operations.
 - By using classical communications, measurement results at one side of EPR pairs are sent to another side of EPR pairs.
 - Correction operations which reflect measurement results are performed on both edges of EPR pairs which are targets of the EPP operations.

Executing this protocol leads to the generation of EPR pairs which are shared between C_0 and C_N .

B. Necessary communications

Quantum communications are needed when EPR pairs are shared between adjacent relay points. These quantum communications are called quantum state transmissions. Classical communications are needed for ES and EPP in all x . We consider classical communications which are used to share measurement results. Therefore, starting points of classical communications are relay points where measurement results are obtained. Destinations of classical communications are relay points where measurement results are used. We have to note that the destinations of communications vary with depending on the operational mode (blind mode execution or ordinary execution) of quantum repeater protocols.

III. BLIND MODE EXECUTION

For keeping high fidelity of EPR pairs which are generated by quantum repeater protocols, it is important to decrease effects of noises during waiting time. The method of execution in the blind mode is proposed as a method for decreasing effects of noises during waiting time.

In the quantum repeater protocol, ES operations and EPP operations are performed. In both of ES operations and EPP operations, we can get desired EPR pairs by performing correction operations which correspond to measurement results. Therefore, correction operations which correspond to measurement results are needed. In blind mode execution[1], the next operation is done without performing correction operations of former operations. In ES, next operations are done before performing correction operations of ES. In EPP, next operations are done before performing correction operations of EPP. Correction operations in ES and EPP are done in a lump after EPR pairs are shared among the sender and the receiver. Thus, we do not have to wait for arrival of classical communications which are used for correction operations.

Execution in the blind mode is possible when quantum states without correction operations are near to one of Bell states. We can continue quantum repeater if targets of operations are near to one of Bell states. Transitions among Bell pairs are one of four Pauli operators. Therefore, we can execute correction operations in a lump. Correction operations at later executions are same as skipped operations.

Blind mode execution in [1] assumes that codes used for EPP are concatenated CSS codes. This is because protocols are continued without correcting errors and errors are accumulated in the blind mode. Therefore, concatenated CSS codes are used for correcting accumulated errors. When CSS codes with single encoding are used without adopting posterior processing in this paper, accumulated errors go over the error correction capability of single code.

IV. PROPOSITION

This section shows our propositions. Execution in blind mode means that correction operations are performed after EPR pairs are shared between the sender and the receiver.

In this algorithm, codes which are used for EPP are CSS codes as in the conventional blind mode[1]. However, the difference is concatenation of CSS codes. Our proposed methods use EPP of single encoding by CSS codes in contrast to conventional methods which use concatenated CSS codes.

First, notations are introduced for explaining the proposed methods. Let $I, \sigma_x, \sigma_z, \sigma_x \sigma_z$ be Pauli operators, which are defined in Appendix A. σ_x corresponds to

an operator of bit errors and σ_z corresponds an operator of phase errors. Let $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$, $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$. These four states are called Bell states. Correction procedures in CSS codes consist of bit error corrections and phase error corrections. Let H_1 be the parity check matrix which is used for bit error correction and H_2 be the parity check matrix which is used for phase error correction. Since methods for bit error corrections and phase error corrections are similar, we describe two corrections at the same time by representing parity matrix as H . Therefore, H is either of H_1 or H_2 . Let $e_{i,ES(j)}$ be base shifts due to Bell measurements which occur on i th qubit at j th ES. Let $\hat{e}_{ES(j)}$ be a vector of base shifts for all qubits which occurred at j th ES. Let $\hat{s}_{EPP(j)}$ be a vector of syndromes which are obtained at j th EPP. A value 1 in error vectors means that an error occurred in the qubit. A value 0 in error vectors means that an error did not occur in the qubit. Syndromes are calculated by multiplying parity check matrices H by error operators. We have to note that syndromes are mapped to error operators by one-to-one mapping if the error operators go under the error correction capability. Let $\sigma_{x,k}^{a_{i,j}}$ be operators of bit errors on i th qubit at j th EPP at the location k and $\sigma_{z,k}^{b_{i,j}}$ be operators of bit errors on i th qubit at j th EPP at the location k . That is, a bit error is caused on i th qubit if $a_{i,j} = 1$ and a phase error is caused on i th particle if $b_{i,j} = 1$. Here, i is the order of qubits within qubits of the same syndrome measurement. That is, i runs from 1 to n (code length). Let k indicates the location of relay point and the location inside the relay point. Let $|\rangle_k$ be quantum states at the k th location. For example, as used in Eq. (2), $k = 1$ indicates the location of the sender and $k = 4$ indicates the location of the receiver and $k = 2$ and $k = 3$ indicate the relay point in the middle of the sender and the receiver. Additionally, $k = 2$ indicates the left side of the middle relay point and $k = 3$ indicates the right side of the middle relay point. We have to note that $\hat{e}_{ES(j)}$ and $\hat{s}_{EPP(j)}$ are computed for the longest EPR pairs which are shared between the sender and receiver by integrating measurement results for multiple sections. The way of integrating is described in the proposed method in this paper.

A. Strategy for blind mode with single encoding

In blind mode, ES operations and EPP operations are performed without waiting for correction operations of the former operations. Therefore, errors of multiple ES operations and multiple EPP operations are accumulated at the last EPP. For quantum repeater protocols of large distance, we cannot estimate large errors by using only syndromes at the last EPP since errors at the last EPP go over the error correction capability. Therefore, we cannot correct errors with simple methods. In this paper, we estimate errors at the last EPP by using syn-

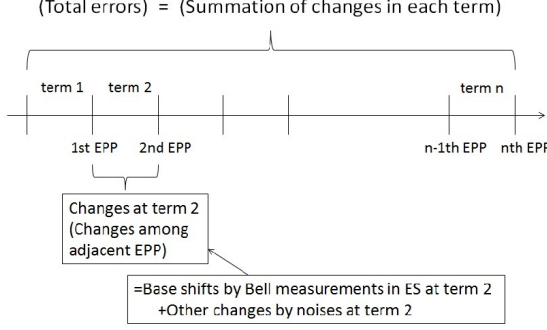


FIG. 1. Decomposition of errors

dromes of the former EPP operations. We estimate by assuming that the final errors are accumulation of errors between EPP operations of adjacent x . Additionally, we assume that each error during EPP operations of adjacent x is under the error correction capability. With these assumptions, we can estimate each error during EPP operations of adjacent x correctly. Besides, we can estimate errors at the last EPP as accumulation of each error during EPP operations of adjacent x . Since syndromes of CSS codes can be calculated as $|H \cdot e\rangle$, we can derive $|H \cdot (e_a + e_b)\rangle - |H \cdot e_a\rangle = |H \cdot e_b\rangle$, where e, e_a, e_b be errors which correspond to the type of H . This equation holds even when the weight of e_a goes over the error correction capability. We can estimate e_b from syndromes if the weight of e_b goes under the error correction capability. It is not necessary that the weight of e_a goes under the error correction capability. This characteristic is true not only for bit error corrections but also for phase error corrections. In the case of phase error corrections, different parity check matrix is used as shown in Appendix A.

This characteristic about syndromes can be used for decomposing errors as the followings. Since syndromes of CSS codes can be calculated as $|H \cdot e\rangle$ (as explained in Appendix A), we can derive $|H \cdot (e_a + e_b)\rangle - |H \cdot e_a\rangle = |H \cdot e_b\rangle$. This equation holds even when the weight of e_a goes over the error correction capability. We can estimate e_b from syndromes if the weight of e_b goes under the error correction capability. It is not necessary that the weight of e_a goes under the error correction capability.

By applying this principle to estimation in quantum repeater protocols, procedures can be described as the followings. For quantum repeater protocols in blind mode, errors are accumulated since corrections are not performed until EPR pairs are shared between the sender and the receiver. For each error during adjacent EPP operations, error operators are $H^{-1}((\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)}))$. By using these operators, accumulated er-

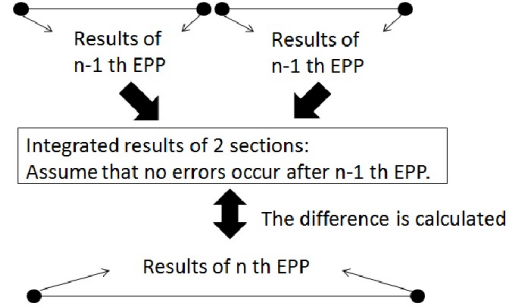


FIG. 2. Adjustments for comparisons

rors can be decomposed as Eq. (1).

$$\begin{aligned}
 & H^{-1}(\hat{s}_{EPP(\gamma)}) \\
 &= H^{-1}((\hat{s}_{EPP(\gamma)} - H \cdot \hat{e}_{ES(\gamma)}) - (\hat{s}_{EPP(\gamma-1)})) \\
 &+ H^{-1}((\hat{s}_{EPP(\gamma-1)} - H \cdot \hat{e}_{ES(\gamma-1)}) - (\hat{s}_{EPP(\gamma-2)})) \\
 &+ \dots \\
 &+ H^{-1}((\hat{s}_{EPP(3)} - H \cdot \hat{e}_{ES(3)}) - (\hat{s}_{EPP(2)})) \\
 &+ H^{-1}((\hat{s}_{EPP(2)} - H \cdot \hat{e}_{ES(2)}) - (\hat{s}_{EPP(1)})) \\
 &+ H^{-1}((\hat{s}_{EPP(1)} - H \cdot \hat{e}_{ES(1)}) - (\hat{s}_{EPP(0)})) \\
 &+ (\hat{e}_{ES(\gamma)} + \hat{e}_{ES(\gamma-1)} + \dots + \hat{e}_{ES(1)}). \quad (1)
 \end{aligned}$$

We have to note that $\hat{s}_{EPP(0)}$ is zero vector since there are no errors at the initial time. As we can see from this equation, overall errors can be described as summation of errors during adjacent EPP operations and base shifts due to ES operations as in FIG. 1. We have to note that this decomposition is possible since syndromes are measured at all EPP operations and Bell measurements are performed at all ES operations. By assuming that the weight of error operators of $H^{-1}((\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)}))$ goes under the error correction capability, we can estimate an appropriate error for each of the intervals. Since measurement results of Bell measurements in ES can be obtained without depending on syndrome measurements in EPP, the number of qubits which are affected by base shifts in ES is not problem. Estimating an appropriate error for each of the intervals and estimating base shifts due to ES operations lead to estimating overall errors by using the equation above.

We have to note that decompositions above are calculated at the points of the sender and the receiver. Additionally, some EPR pairs stay on different sections. Therefore, we have to make arrangements of EPR pairs in order to make comparisons at the points of the sender and the receiver. We explain about the case of comparing EPP at $x = i$ and EPP at $x = j$, where $i < j$.

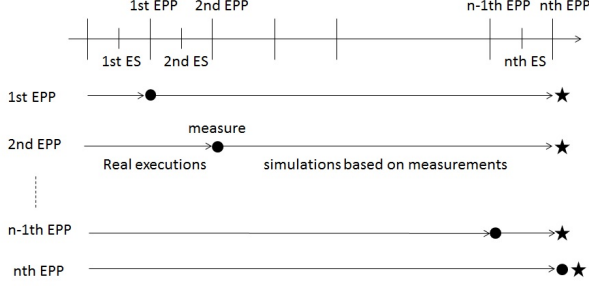


FIG. 3. Real execution and simulation

Since the length of EPR pairs are different between $x = i$ and $x = j$, locations where measurement results are obtained are different. The measurement results in EPP at $x = i$ are processed by ES and EPP until x reaches j . This processing is performed by assuming that no errors occur after EPP at $x = i$. We have to note that this processing can be performed with simulations in classical computers by using measurement results of EPP at $x = i$. After measurement results at $x = i$ are processed by simulations and values at $x = j$ are calculated, we can compare two values since both values are for $x = j$. FIG. 2 shows an example of comparing EPP at $x = n - 1$ and EPP at $x = n$. FIG. 3 shows the way of comparing measurement results of EPP at all x by processing each of the measurement results until each x reaches n . In FIG. 3, for each EPP, measurements are performed at the point of the circle and measurement results are processed by simulations from the point of the circle to the point of the star. Thus, all measurement results of EPP at different x can be compared as the longest EPR pairs.

For integrating base shifts in ES operations into one base shift which corresponds to an EPR pair shared between the sender and the receiver, we use the same methods. We integrate results of base shifts for x th ES operations in multiple sections by executing quantum repeater protocols with assuming that no errors occur after x th ES operations.

B. Outline of the proposed algorithm

The proposed algorithm sets some assumptions about noises. These assumptions are fair in comparing between the proposed methods and the conventional methods, which is the blind mode execution with concatenated coding. This paper takes channel noises and memory noises into consideration. Additionally, this paper assumes that noises in ES operations and EPP operations

and measurements lead only to degradation of fidelity. However, this paper does not take some failures into consideration, such as photon losses and unexecution of operations and delay of operations. Estimations in this paper are calculated under these assumptions.

First, we describe the procedure transmission stage of the algorithm. In this stage, we use classical communications for conveying the procedure of the quantum repeater protocol. It is not problem to use classical communications in this stage since EPR pairs are not generated in this stage and we do not have to care about effects of quantum memory noise.

- The sender decides the procedure of the quantum repeater protocol. The procedure consists of multiple commands. Each command consists of an ID of a relay point, a time and an operation at the time on the relay point. The procedure tells each relay point to execute the indicated operation at the indicated time.
- The sender sends the procedure to all relay points.

Each of the relay points execute the indicated operations at the indicated time without knowing situations of other relay points. Therefore, classical communications are not needed between the time of generating EPR pairs and the time of finishing sharing EPR pairs.

After the procedure is shared among all relay points, ES operations and EPP operations are executed as the following. Since CSS codes of single encoding are used in this protocol, ES operations at all x and EPP operations at all x are performed on n EPR pairs. Here, n is the code length of CSS codes of single encoding.

- In each relay point, C_i ($i = 0, \dots, N - 1$), n Bell states are generated, where n is the code length of a CSS code of single encoding. An example of the states are $|\phi^+\rangle^{\otimes n}$. (If the required code is different from natural Bell states, Bell states are encoded by measuring with measurement operators of a CSS code as in [14]. These measurements lead to convergence into an eigenspace (see Appendix A). Transformations into another eigenspace are performed if specific eigenspace is required.)
- Then, one side of each EPR pair is sent from C_i to C_{i+1} .
- From $x = 1$ to $x = \gamma$, repeat the following operations. ES and EPP are performed right after the preceding operation is finished. That is, operations are performed without waiting for arrivals of classical communications. Since this algorithm considers blind mode, only measurements are performed at this stage and correction operations which correspond to measurement results are performed at the later stage.
 - Bell measurements of ES are performed on relay points, $C_{k \times 2^{x-1}}$ ($k = 1, 2, \dots, N/2^{x-1} - 1$)

except $C_{2^x}, C_{2 \times 2^x}, \dots, C_{N-2^x}$. These operations lead to generation of EPR pairs which are shared between $C_{k \times 2^x}$ and $C_{(k+1)2^x}$ for $k = 0, \dots, N/2^x - 1$.

- Measurement results at relay points where ES are performed are sent to the sender and the receiver.
- Syndrome measurements of EPP are performed at edges of EPR pairs, $C_{k \times 2^x}$ and $C_{(k+1)2^x}$ for $k = 0, \dots, N/2^x - 1$. Operators of syndrome measurements at these EPP operations correspond to those of CSS codes as in [14].
- Measurement results at relay points where EPP are performed are sent to the sender and the receiver.

After all ES operations and all EPP operations are finished, we estimate correction operations based on measurement results as the followings. The detail of calculation of correction operations are shown in the next subsection. This subsection shows summary of calculating correction operations. In this algorithm, we assume that all ES operations and all EPP operations are performed as scheduled.

- The sender and the receiver wait for signals of measurement results in ES and EPP.
- FOR each EPR pair
 - We calculate correction operations for ES operations at each x . We also calculate correction operations for EPP operations separately from those of ES operations. This separated calculation is done by using relationship in Eq. (1).
 - Correction operations which correspond to ES operations on the EPR pair are calculated as the followings. This calculation corresponds to calculating the latter part of the right side of Eq. (1).
 - * For each x , multiple EPR pairs stay on multiple sections. Since correction operations are performed on EPR pairs which are shared between the sender and the receiver, correction operations for multiple sections have to be integrated into one correction operation for each x . This integration is done by using Eq. (2) and Eq. (3).
 - Correction operations which correspond to EPP operations on the EPR pair are calculated as the followings. This calculation corresponds to calculating the former part of the right side of Eq. (1).

- * For each x , syndromes of multiple EPR pairs are summarized into one syndrome which correspond to EPR pairs shared between the sender and the receiver. This integration can be explained as in FIG. 2 and FIG. 3.
- * For each x , the difference of syndromes are calculated between EPP at x and EPP at $x + 1$. Then, correction operations are estimated for each term in FIG. 1. We have to note that effects of base shifts in ES operations can be removed in calculating this difference since base shifts due to ES operations are calculated as described above.
- * Overall errors except base shifts due to ES are estimated by accumulating all of the decomposed errors as in FIG. 1.
- For each EPR pair, we perform correction operations which are computed by procedures above. Correction operations in ES and correction operations in EPP can be correlated as in Eq. (1). We have to note that we compute correction operations for each of bit error corrections and phase error corrections.

• END FOR

We have to note that procedures above are performed for bit error corrections and phase error corrections separately. Parity check matrix in bit error correction is different from parity check matrix in phase error correction.

C. Calculation of correction operations

Correction operations which are used in the algorithm above are calculated as the followings.

Correction operations for ES are calculated as the followings. In Bell measurements for connections, measurement results which correspond to base shifts are obtained. Correction operations for ES are operators of base shifts, which are one of four Pauli operators. Since correction operations are performed on EPR pairs which are shared between the sender and the receiver, correction operations for multiple sections have to be integrated into one correction operation for each x . The way of integrations into one correction operation is similar to that in EPP and can be described by applying Eq. (3), which are explained in detail in the following.

Correction operations for EPP are calculated as the followings. First, we explain a calculation of the primitive case. Complex calculations can be done by repeating this calculation. Correction operations which are specific to j th EPP are calculated by subtracting syndromes at $j - 1$ th EPP and syndromes at j th ES from syndromes at j th EPP. That is, the correction operations are operators which correspond to $(\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)})$.

In short, correction operations for j th ES are $\hat{e}_{ES(j)}$ and correction operations for j th EPP are operations which correspond to $(\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)})$.

We have to note that $(\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)})$ are calculated at both edges of EPR pairs of j th EPP. This can be explained as the followings. Connection of Bell states can be described as

$$\begin{aligned} & |\phi^+\rangle_{1,2} |\phi^+\rangle_{3,4} \\ &= |\phi^+\rangle_{1,4} |\phi^+\rangle_{2,3} + |\phi^-\rangle_{1,4} |\phi^-\rangle_{2,3} \\ &+ |\psi^+\rangle_{1,4} |\psi^+\rangle_{2,3} + |\psi^-\rangle_{1,4} |\psi^-\rangle_{2,3}. \end{aligned} \quad (2)$$

Eq. (2) means that Bell measurements on particle 2 and 3 lead to convergence into one of four Bell states on particle 1 and 4. Besides, Bell states on particle 2 and 3 correspond to Bell states on particle 1 and 4. Therefore, we can know which EPR pairs are obtained at particle 1 and 4 by watching states on particle 2 and 3. Performing Pauli operators on the left side of Eq. (2) leads to the following equation for each i ($i = 1, \dots, n$).

$$\begin{aligned} & (\sigma_{x,1}^{a_{i,j-1}} \sigma_{z,1}^{b_{i,j-1}} \sigma_{x,2}^{a_{i,j-1}} \sigma_{z,2}^{b_{i,j-1}}) |\phi^+\rangle_{1,2} \\ & \otimes (\sigma_{x,3}^{a_{i,j-1}} \sigma_{z,3}^{b_{i,j-1}} \sigma_{x,4}^{a_{i,j-1}} \sigma_{z,4}^{b_{i,j-1}}) |\phi^+\rangle_{3,4} \\ &= (\sigma_{x,1}^{a_{i,j-1}} \sigma_{z,1}^{b_{i,j-1}} \sigma_{x,4}^{a_{i,j-1}} \sigma_{z,4}^{b_{i,j-1}} \\ & \otimes \sigma_{x,2}^{a_{i,j-1}} \sigma_{z,2}^{b_{i,j-1}} \sigma_{x,3}^{a_{i,j-1}} \sigma_{z,3}^{b_{i,j-1}}) \\ & \times (|\phi^+\rangle_{1,4} \otimes |\phi^+\rangle_{2,3} + |\phi^-\rangle_{1,4} \otimes |\phi^-\rangle_{2,3} \\ & + |\psi^+\rangle_{1,4} \otimes |\psi^+\rangle_{2,3} + |\psi^-\rangle_{1,4} \otimes |\psi^-\rangle_{2,3}). \end{aligned} \quad (3)$$

The left side of Eq. (3) means EPR pairs before connections. The right side of Eq. (3) has 4 terms. Each of the 4 terms corresponds to EPR pairs after connection. $\hat{s}_{EPP(j-1)}$ means syndromes which correspond to $\sigma_{x,1}^{a_{i,j-1}} \sigma_{z,1}^{b_{i,j-1}} \sigma_{x,4}^{a_{i,j-1}} \sigma_{z,4}^{b_{i,j-1}}$ of all i . $\hat{e}_{ES(j)}$ means operators which change states after Bell measurements on particle 1 and 4 into the desired term of the right side of Eq. (3). Therefore, $\hat{e}_{ES(j)}$ changes a Bell state to another Bell state. $\hat{s}_{EPP(j)}$ means syndromes which correspond to $\sigma_{x,1}^{a_{i,j}} \sigma_{z,1}^{b_{i,j}} \sigma_{x,4}^{a_{i,j}} \sigma_{z,4}^{b_{i,j}}$ of all i . When changes occur only by Bell measurements, error operators satisfy $\sigma_{x,1}^{a_{i,j-1}} \sigma_{z,1}^{b_{i,j-1}} \sigma_{x,4}^{a_{i,j-1}} \sigma_{z,4}^{b_{i,j-1}} = \sigma_{x,1}^{a_{i,j}} \sigma_{z,1}^{b_{i,j}} \sigma_{x,4}^{a_{i,j}} \sigma_{z,4}^{b_{i,j}}$ for all i . However, due to other noises, errors are not only shift changes at ES. Therefore, error operators at EPP(j) can be different from error operators at EPP(j-1). By using Eq. (3), we can compute correction operations for each ES and EPP. In other words, we can integrating errors of multiple EPP(j-1) into one errors on longer EPR pairs by processing quantum repeater protocols with assuming that no errors occur after EPP(j-1).

For estimating overall errors, we summarize the decomposed errors. Since the longest EPR pairs in protocols are shared between the sender and the receiver, we compute the difference of adjacent EPP operations by integrating shorter EPR pairs into the longest EPR pairs, which are shared between the sender and the receiver. We can integrate errors for each section into errors of larger sections

as in the calculation of the primitive case above and FIG. 2. Repeating these integrations lead to computing integrated errors on EPR pairs shared between the sender and the receiver. The methods of computing the differences are shown in FIG. 3.

V. PERFORMANCE OF THE PROPOSED PROTOCOLS

This section compares the difference between the conventional blind mode and the proposed method. As stated in the introduction of this paper, the main focus of this paper is posterior processing of measurement results. Therefore, it is appropriate to compare with protocols which focus on posterior processing. Even if some specifications are inferior to those of protocols which focus on encoding, it is not problem since focuses are different. Improvements in the proposed method may be used for posterior processing part of protocols which focus on encodings and can enhance specifications of protocols which focus on encodings. Additionally, since propositions in this paper focus on posterior processing of measurement results, the most important thing which we should analyze is correctness of estimating correction operations and conditions for the correctness. We suppose that correction operations are estimated after EPR pairs are shared between the sender and the receiver by using measurement results which are obtained before EPR pairs are shared between the sender and the receiver. Therefore, we have to check that estimation of correction operations is valid even after the following ES operations and EPP operations are performed.

This paper sets some assumptions about noises. These assumptions are fair in comparing between the proposed methods and the conventional blind mode. This paper takes channel noises and memory noises into consideration. Additionally, this paper assumes that noises in ES operations and EPP operations and measurements lead only to degradation of fidelity. However, this paper does not take some failures into consideration, such as photon losses and unexecution of operations and delay of operations. Estimations in this paper are calculated under these assumptions.

A. Correctness of estimation

Since operators for measuring syndromes in EPP correspond to those of CSS codes, EPP has a parameter of the error correction capability, which are denoted as t . We can specify errors as long as the weight of an error is less than t since an error and syndromes can be mapped by one-to-one mapping in this case. Therefore, we can trace accumulation of errors if the weight of each error during each interval of syndrome measurements is less than t qubits. This means that we can specify errors even when the weight of accumulated errors goes over t ,

if the weight of an error during each interval of syndrome measurements is less than t .

By applying this method to quantum repeater protocols, we can correct errors of large weight if we measure syndromes at each EPP and if the weight of each error during adjacent EPP operations is less than t . This is the new assumption which is needed for blind mode with single encoding.

Additionally, since base shifts due to ES operations can be detected and corrected without dependence on errors in EPP, the number of qubits which are affected by base shifts due to ES is not problem. Therefore, correcting large errors is possible if the weight of an error which corresponds to $(\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)})$ are less than t for each j in both of bit error corrections and phase error corrections.

Correctness of this estimation can be shown by decomposing accumulated errors as follows. Overall errors can be decomposed by using Eq. (1). As we can see from this equation, overall errors can be described as summation of errors during adjacent EPP operations and base shifts due to ES operations as in FIG. 1. By assuming that the weight of error operators of $H^{-1}((\hat{s}_{EPP(j)} - H \cdot \hat{e}_{ES(j)}) - (\hat{s}_{EPP(j-1)}))$ goes under the error correction capability, we can estimate an appropriate error for each of the intervals since an error and a syndrome can be mapped by one-to-one mapping in this case. Additionally, since measurement results of Bell measurements in ES can be obtained without depending on syndrome measurements in EPP, the number of qubits which are affected by base shifts in ES is not problem. Estimating an appropriate error for each of the intervals and estimating base shifts due to ES operations lead to estimating overall errors by using Eq. (1). Discussions above show that correction operations match if the weight of an error between adjacent EPP operations goes under the error correction capability. Since the proposed protocol does not consider photon losses and unexecutions of operations, nonexistence of these errors are assumed.

B. Inheritance of major merits

This subsection shows that the proposed protocol could reduce resources without spoiling major merits of the conventional blind mode. We have to note that minor points of the conventional blind mode are changed. That is, additional assumptions about frequency of errors are changed, as described in the previous section.

What we could improve in the proposed method is the number of EPR pairs which are used in the protocol. The number of EPR pairs in the conventional method is $N * n^\gamma$. The number of EPR pairs in the proposed method is $N * n$. This is because the proposed protocol could execute by using CSS codes with single encoding.

Although the proposed protocol could reduce resources, the proposed protocol inherits major merits of the conventional blind mode.

- One of the merits in the conventional blind mode is smallness of waiting times. The expected time of executing protocols is as follows. The time for executing the conventional method is almost same as the time for executing the proposed method. Both of the time above are the summation of the time of delivering EPR pairs to adjacent nodes and the time of executing ES operations and EPP operations since these protocols are executed in the blind mode. The time for classical communications of sending measurement results are not considered since this time does not affect the fidelity of generated EPR pairs.
- The other merit of the conventional blind mode is sending small states via channels by using EPP in [14]. For example, one side of $|\phi^+\rangle^{\otimes n}$ are sent via channels in the EPP. In both of the conventional blind mode and the proposed blind mode, quantum states which are sent via channels can be small EPR pairs, such as isolated $|\phi^+\rangle$, by using the EPP[14].
- Another point of comparison is adjustments to errors. The type of errors to which the proposed protocol adjust is almost same as the type of errors to which the conventional protocol adjust. The type of errors is degradation of EPR pairs in channel transmissions and in ES operations and noises during waiting times. Both of the proposed method and the conventional method could adjust to these errors as long as errors are within the error correction capability of entanglement purification. The small difference is setting additional assumptions in the proposed method. The assumption is that each of the errors during adjacent EPP operations goes under the error correction capability. The detail of this assumption is explained in the previous section.

However, the proposed protocol and the conventional blind mode did not consider photon losses and unexecution of operations.

Thus, we could show that the proposed protocol could reduce resources without spoiling merits of the conventional blind mode except the new assumption above.

The results of this paper show that posterior processing of measurement results can reduce the size of encoded states with keeping high correction capability. Since one of the hurdles against realization of some quantum repeater protocols is largeness of encoded states, essence in this paper will be useful for reducing the size of the encoded states by improving posterior processing of measurement results.

VI. CONCLUSION

We constructed concrete methods of blind mode with single encoding. Our proposed methods do not use con-

catenated CSS codes, but use single encoding by CSS codes. We showed that the proposed method can correct large errors by using CSS codes of single encoding if overall errors are decomposed and each of the decomposed errors goes under the error correction capability. The results of this paper show that posterior processing can improve performance of error corrections in comparison with the conventional blind mode with single encoding. The proposed protocol with single encoding can correct large errors by setting some assumptions. In contrast, blind mode with single encoding can deal with small errors if propositions in this paper are not used. In other words, the results of this paper show that posterior processing can reduce the size of encoded states in comparison with the conventional blind mode with concatenated codes. In summary, the proposed way about posterior processing is effective for improving performance of error corrections and for reducing the size of encoded states.

Appendix A: CSS codes and EPP

In this section, we explain CSS codes[17] and its conversion to EPP[14][18].

1. Code construction and error representation

Since CSS codes are subclass of stabilizer codes, CSS codes inherit characteristics of stabilizer codes. First, I describe stabilizer codes. Then, I describe CSS codes as special cases of stabilizer codes. Possible errors can be represented as superposition of some error bases. These bases belong to a group, which is called as the error group. In order to construct the error group, we define Pauli operators as in Eq. (A1).

$$\begin{aligned} I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \sigma_x \sigma_z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \end{aligned} \quad (\text{A1})$$

By using Eq. (A1), the error group can be written as

$$\begin{aligned} E^n &= \{\pm M_1 \otimes M_2 \otimes \cdots \otimes M_n \mid \\ M_1, \dots, M_n &\in \{I, \sigma_x, \sigma_z, \sigma_x \sigma_z\}\}. \end{aligned} \quad (\text{A2})$$

We describe elements of the error group as $E_i^n = E_i^{n|1} \otimes E_i^{n|2} \otimes \cdots \otimes E_i^{n|n}$, where $E_i^{n|1}, \dots, E_i^{n|n}$ are one of 4 Pauli operators. Codewords of stabilizer codes are elements of eigenspaces of subgroups of the error group. Let a subgroup of the error group be P . Codewords are elements of an eigenspace of P . An eigenspace means a space of states which have the same eigenvalue for all operators in P .

There are some methods for representing quantum errors such as methods by state vectors and methods by

density operators. In this paper, we describe the change of state vectors. Let $|\Psi\rangle$ be a codeword of stabilizer codes. Quantum states of n qubits change by unitary operators as the following.

$$\begin{aligned} U_n |\Psi\rangle &= \sum_i (c_i E_i^n |\Psi\rangle) = \\ &\sum_{i,j} c_{i,j} E_i^m |\psi\rangle \otimes E_j^{n-m} |\phi\rangle. \end{aligned} \quad (\text{A3})$$

Here, $E_i^n \in E^n$. $|\Psi\rangle$ consists of n qubits. Let m qubits out of the n qubits be system and be described as $|\psi\rangle$. Let the other $n - m$ qubits be environment and be described as $|\phi\rangle$. Setting $\sum_j c_{i,j} E_j^{n-m} |\phi\rangle = \nu_i$ and outputting syndromes a_i into ancilla leads to

$$U_n |\Psi\rangle = \sum_i E_i^m |\psi\rangle \otimes \nu_i \otimes |a_i\rangle. \quad (\text{A4})$$

Measuring ancilla leads to

$$E_i^m |\psi\rangle \otimes \nu_i \otimes |a_i\rangle. \quad (\text{A5})$$

Measuring ancilla of Eq. (A4) leads to conversion into Eq. (A5). Eq. (A5) represents codewords which are affected by one of error bases. Thus, measuring ancilla leads to conversion into bases of errors. Then, we can specify errors on codewords.

2. Error correction capability

We define the weight of E_i^n in the following. Let this weight be $\gamma(E_i^n)$. E_i^n consists of tensor products of n Pauli operators (Eq. (A1)). The weight of E_i^n means the number of operators which are not I out of n operators. Stabilizer codes of minimum distance θ can correct error bases whose weight goes under $\lfloor(\theta - 1)/2\rfloor$. Thus, stabilizer codes of minimum distance θ can correct errors which occurred on less than $\lfloor(\theta - 1)/2\rfloor$ qubits. This parameter is called the error correction capability.

3. Codes construction of CSS codes

In CSS codes, codewords $|\Psi\rangle$ are constructed as follows. Suppose C_1 and C_2 are $[n, k_1]$ and $[n, k_2]$ classical linear codes such that $C_2 \subset C_1$ and C_1 and C_2^\perp both correct t errors. By using the C_1 and C_2 , CSS code can be constructed as $|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$, where $x \in C_1$ is any codeword in C_1 . Let H_1 be parity check matrix of C_1 and H_2 be parity check matrix of C_2 . Then, syndromes of CSS codes correspond to $|H_1 \cdot e_1\rangle$ for bit error corrections and $|H_2 \cdot e_2\rangle$ for phase error corrections. That is, states after outputting syndromes of bit error e_1 are $|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y + e_1\rangle |H_1 \cdot e_1\rangle$.

4. Algorithms for error correction

In the error correction stage, we perform unitary operators to output syndromes on ancilla. We specify errors based on syndromes which are measured on ancilla. Operators to output syndromes are decided by the subgroup P . In CSS codes, these operators can be divided into two categories. One is for bit error detection and another is for phase error detection. Therefore, in CSS codes, the error correction stage can be divided into the bit error correction stage and the phase error correction stage. The phase error correction stage is executed by performing WH translations before measuring syndromes and correcting errors. WH translations are performed again after correcting phase errors.

5. Conversion to EPP

Concrete methods of general conversion into EPP are written in [14],[18] as summarized in the followings.

- Alice prepares multiple Bell states. The number of Bell states corresponds to the code length. (If the required code is different from natural Bell states, Alice encodes these Bell states by measuring with measurement operators of stabilizer codes or CSS codes.)
- Alice sends one side of each EPR pair to Bob.
- Alice and Bob measure syndromes by using measurement operators which correspond to those of stabilizer codes or CSS codes.
- Alice and Bob exchange syndrome information and specify errors based on syndrome information.

As above, measurement operators in EPP correspond to those of stabilizer codes or CSS codes. Thus, EPP can correct errors when the number of error qubits goes under the error correction capability.

-
- | | |
|---|--|
| <p>[1] H.Hartmann, B.Kraus, H.Briegel, and W.Dur, Phys.Rev.A 75, 032310 (2007).</p> <p>[2] W.Dur, H.Briegel, J.Cirac, and P.Zoller, Phys.Rev.A 59, 169 (1999).</p> <p>[3] L.M.Duan, M.D.Lukin, J.I.Cirac, and P.Zoller, Nature 414, 413 (2001).</p> <p>[4] P.V.Loock, T.D.Ladd, K.Sanaka, F.Yamaguchi, K.Nemoto, W.J.Munro, and Y.Yamamoto, Phys.Rev.Lett 96, 240501 (2006).</p> <p>[5] J.B.Brask, I.Rigas, E.S.Polzik, U.L.Andersen, and A.S.Sorensen, Phys.Rev.Lett 105, 160501 (2010).</p> <p>[6] L.Childress, J.M.Taylor, A.S.Sorensen, and M.D.Lukin, Phys.Rev.A 96, 070504 (2006).</p> <p>[7] L.Jiang, J.M.Taylor, K.Nemoto, W.J.Munro, R.Meter, and M.D.Lukin, Phys.Rev.A 79, 032325 (2009).</p> <p>[8] M.Razavi, M.Piani, and N.Lutkenhaus, Phys.Rev.A 80, 032301 (2009).</p> | <p>[9] P.Mazurek, A.Grudka, M.Horodecki, P.Horodecki, J.Lodyga, L.Pankowski, and A.Przysieczna, Phys.Rev.A 90, 062311 (2014).</p> <p>[10] Y.Li, S.D.Barrett, T.M.Stace, and S.C.Benjamin, New J. Phys. 15, 023012 (2013).</p> <p>[11] K.Azuma, K.Tamaki, and H.K.Lo, Nature Communication, 7787 (2015).</p> <p>[12] M.Zwerger, W.Dur, and H.J.Briegel, Phys.Rev.A 85, 062326 (2012).</p> <p>[13] C.H.Bennett, D.P.Divincenzo, J.A.Smolin, and W.K.Wootters, Phys.Rev.A 54, 3824 (1996).</p> <p>[14] P.W.Shor and J.Preskill, Phys.Rev.Lett. 85, 441 (2000).</p> <p>[15] C.H.Bennett, G.Brassard, C.Crepeau, R.Jozsa, A.Peres, and W.K.Wootters, Phys.Rev.Lett. 70, 1895 (1993).</p> <p>[16] M.Varnava, D.E.Browne, and T.Rudolph, Phys.Rev.Lett. 97, 120501 (2006).</p> <p>[17] A.Calderbank and P.Shor, Phys.Rev.A 54, 1098 (1996).</p> <p>[18] R.Matsumoto, Journal of Physics A 36, 8113 (2002).</p> |
|---|--|